2B-4

モデル検査における検査対象と外部環境の自動合成手法

藤本 宏† 森 奈実子† 村田 由香里†
株式会社 東芝 ソフトウェア技術センター†

1. はじめに

近年，ソフトウェアの複雑化や大規模化が一段と進み，その適用領域は広がり続けている．これに伴い，ソフトウェア起因の不適合による社会的影響が大きくなっており，ソフトウェアの機能的な品質だけでなく，信頼性や安全性の側面からの品質向上もこれまで以上に求められるようになりつつある．

ソフトウェアの品質向上に有効な技術としてモデル検査がある．モデル検査は，システムの振る舞いについて網羅的な自動検査が可能な技術である．モデル検査では，検査式として与えられたシステムが満たすべき条件に対して，条件に違反する振る舞いが発生しないことを検査できる．

筆者らは，これまでにモデル検査の適用を容易化するモデル検査自動化ツール[1]を開発した．このツールを用いると，図 1 に示すように検査対象の動作仕様をモデル化した状態遷移表を入力として，モデル検査を自動実行することが可能である．

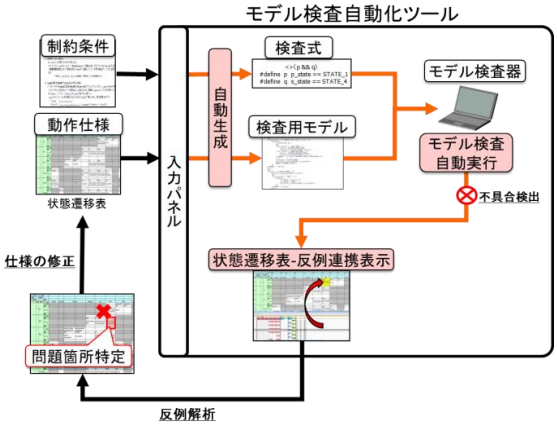

図 1 モデル検査自動化ツール

しかし，モデル検査の適用においては，検査対象の動作仕様に加え，検査対象のシステムに影響を与えるシステム外(外部環境)の要因についてもモデル化する必要がある．外部環境のモデル化は，検査対象とは別に外部環境の振る舞い自体をモデル化する方法が一般的である．しかしこの方法では，外部環境の動作仕様を状態遷移モデルなどを用いてモデル化する作業が新たに発生し，また外部環境自体の振る舞いが検査に加わる事から状態の組合せ爆発が発生しやすくなるという問題があり，モデル検査の適用を妨げる要因となっていた．

本稿では，この外部環境のモデル化について，新たに状態遷移モデルなどを作成する作業を不要とし，検査対象に影響を与える外部環境を宣言的に記述，それを検査対象のモデルへ合成する手法について述べる．

2. 提案手法

外部環境のモデル化は，従来の方法では図 2 に示すように，検査対象に影響を与える外部環境の要因を検査対象が参照する変数と捉え，その取りうる値の種類を状態に，値を変化させるトリガをイベントとすることで，外部環境の動作仕様を状態遷移表としてモデル化していた．これらの状態遷移表を入力としてモデル検査を実行すると，全ての状態の組み合わせにおいて，全てのイベントが発生する場合の振る舞いが検査され，外部環境を含めた網羅的な振る舞いの検査となる．

検査対象の動作仕様

状態＼イベント	E1	E2	E3	E4
S1	S2			S3
S2		S3	S1	S1
S3	S2 α=Ex			S1 α=Ex

外部環境の動作仕様

状態＼イベント	E5	E6
Ex=1		Ex=5
Ex=5	Ex=1	

値変化のトリガ

外部環境がとりうる値の種類

図 2 外部環境のモデル化(従来の方法)

提案手法では，外部環境のモデル化において外部環境自体の振る舞いをモデル化の対象に含める必要は無いという点に着目した．これは，モデル検査で必要となるのは，検査対象の全ての振る舞いが検査されることであり，そのためには検査対象に影響を与える外部環境の要因が全て網羅されていることと，その外部環境の全ての要因について検査対象の振る舞いが検査されていれば良いということである．

そこで，提案手法では外部環境のモデルとして状態遷移表を作成するのではなく，変数宣言としてのみ外部環境をモデル化し，それを以下

Automatic Integration of the External Environment to the Design Model in Model Checking.
Hiroshi Fujimoto†, Namiko Mori†, Yukari Murata†
†TOSHIBA Corporation Software Engineering Center

の手順で検査対象に合成することとした．(図 3)
① 外部環境を，検査対象が参照する変数とそのとりうる値として記述する
② 検査対象のモデルである状態遷移表から，外部環境である変数を参照している箇所を抽出する
③ 抽出した箇所に，その変数が取りうる値それぞれの場合の処理分岐を作成する
この合成結果のモデルを用いてモデル検査を実行すると，検査対象が外部環境の影響を受ける箇所では，外部環境の値それぞれについて振る舞いを検査する実行系列が生成される．つまり，外部環境の全ての要因について検査対象の振る舞いが検査されるということである．

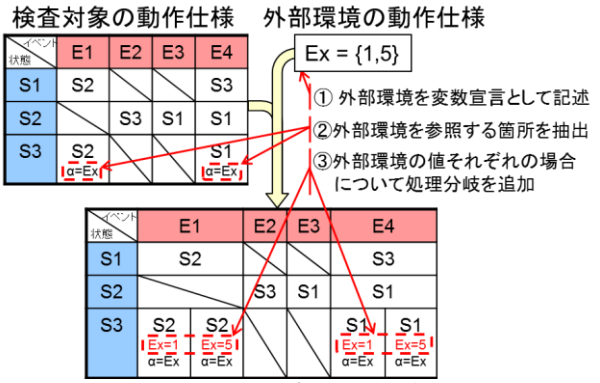

図 3　外部環境のモデル化(提案手法)

3.　提案手法の効果と評価

モデル検査の実行時に生成される遷移の実行系列を用いて，提案手法の効果を示す．従来の方法で外部環境をモデル化した場合，モデル検査の実行時には図 4 のような遷移の実行系列が生成される．この方法では，外部環境の動作が連続する実行系列や，検査に影響しないタイミングで外部環境が動作する実行系列といった，検査対象の検査に不要な遷移が生成され，状態の組合せ爆発の一因となっている．

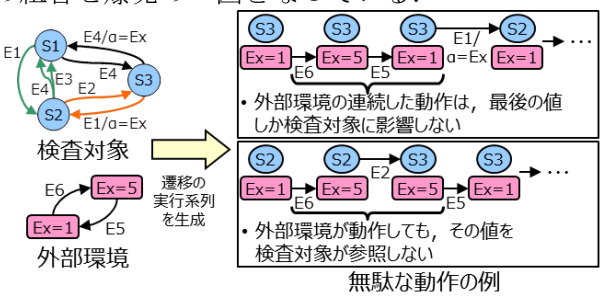

図 4 生成される遷移の実行系列(従来の方法)

これに対し，提案手法で外部環境をモデル化した場合は，図 5 のような遷移の実行系列が生成される．この方法では，外部環境の動作が連続するといった，検査対象の検査に不要な遷移は発生せず，遷移数の増加を抑制することができる．

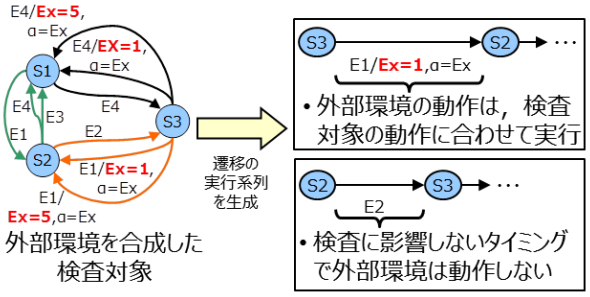

図 5 生成される遷移の実行系列(提案手法)

提案手法の手順②と③に相当する処理をモデル検査自動化ツールに組み込み，提案手法の効果を評価した．表 1 の規模の検査対象に対して，従来の方法と提案手法のそれぞれでモデル検査を実行した結果は表 2 に示すように，探索の遷移数が約 1/10，メモリ使用量が約 1/2 となった．この評価結果より，外部環境を含めた検査において提案手法は状態の組合せ爆発の抑制に有効だと確認できた．

表 1　検査対象の規模

	状態数(個)	イベント数(個)	遷移数(個)
検査対象	10	14	467
外部環境	2	3	3

表 2　モデル検査の実行結果

	探索の遷移数(個)	メモリ使用量(Mbyte)
従来の方法	86,684,846	1,163.475
提案手法	7,656,871	501.659

4.　おわりに

本稿では，モデル検査の適用において必要となる外部環境のモデル化において，変数と取りうる値の宣言的な記述というモデル化方法を用いることで，状態の組合せ爆発の発生を抑制しつつ，検査対象へ合成する手法について述べた．

モデル検査はソフトウェアの品質向上に有効な技術であるが，習得コストの高さや追加作業の必要性により，未だ適用は部分的である．今後もモデル検査の適用範囲を広げるための手法をさらに検討していく．

参考文献

[1] 高田沙都子, 森奈実子, 村田由香里:モデル検査自動化ツールの開発～検査自動化と反例解析効率化～, 情報処理学会 第 74 回全国大会(2012)